

Serial No. : 09/992,831**Patent
Docket No. 156906-0010**

discussing the instant application during a brief telephonic interview. Based on those discussions, as detailed in the Remarks below, it is believed that claims 1-2 and 11 also presently stand in condition for allowance. Furthermore, without acquiescence in the grounds of the rejection, and without prejudice to pursue at a later time, Applicant has canceled claim 6, rewritten claims 16, 17 and 21 in independent form, and amended independent claim 18 to reflect subject matter of claim 1 which, as noted, should be allowable. The Examiner indicated that these amendments should place all of claims 1-2 and 11-22 in condition for final allowance.

In addition, a terminal disclaimer has been filed herewith, to preempt any potential obviousness-type double patenting issue and expedite prosecution of this application.

Accordingly, please amend this application as shown herein. In view of the amendments and accompanying remarks, reconsideration of the present rejection is respectfully requested.

Summary of Claims

Pending: 1-2, 6, 11-22

Amended: 16, 17, 18, 21

Unchanged: 1-2, 11-15, 19-20, 22

Canceled: 6

Amendments to the Claims are reflected in the listing of claims which begins on page 3 of this paper.

Remarks begin on page 11 of this paper.

Serial No. : 09/992,831**Patent
Docket No. 156906-0010****AMENDMENTS TO THE CLAIMS**

Please cancel claim 6, and amend claims 16, 17, 18 and 21 with the following amended versions thereof, without acquiescence in the grounds of rejection and without prejudice to pursue the original claims at a later time by continuation application or otherwise.

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS

1. (Previously Presented) A security device for use in a cashless system wherein portable data devices may be used to conduct cashless transactions, comprising:

a data device reader adapted to receive and read portable data devices;

a host device physically proximate to said data device reader, said host device comprising a host device processor; and

a security module interposed between said data device reader and said host device processor and uniquely identified with said host device, said security module preventing completion of a transaction involving said data device reader and said host device processor unless said data device reader is successfully cross-authenticated with said security module when a portable data device is presented to and read by said data device reader, independent of any authentication of said portable data device by said data device reader.

Serial No. : 09/992,831

Patent
Docket No. 156906-0010

2. (Previously Presented) The security device of claim 1, wherein said portable data devices comprise smart cards, and wherein said data device reader comprises a smart card reader.

3.-10. (Canceled)

11. (Previously Presented) The security device of claim 1, wherein said host device comprises an electronic gaming machine, and wherein said host device processor controls the electronic gaming machine.

12. (Previously Presented) The security device of claim 1, wherein, in addition to cross-authentication between said data device reader and said security module, said data device reader performs a cross-authentication check with the portable data device when it is presented to and read by said data device reader, and prevents a transaction with the portable data device if the cross-authentication check fails.

13. (Previously Presented) The security device of claim 12, wherein said data device reader further comprises an internal security access module, said internal security access module adapted to automatically perform cross-authentication between said portable data device and said data device reader, and

Serial No. : 09/992,831**Patent
Docket No. 156906-0010**

to automatically perform cross-authentication between said data device reader and said security module.

14. (Previously Presented) The security device of claim 13, wherein said security module is configured to perform periodic authentication of said data device reader after the successful cross-authentication between said data device reader with said security module, and to prevent further communication between said data device reader and said host device processor if the periodic authentication fails.

15. (Previously Presented) The security device of claim 13, wherein said internal security access module is adapted to generate a first random number, encipher said first random number using a common key to generate a first enciphered random number, send said first enciphered random number to said security module, receive a second enciphered random number from said security module, decipher said second enciphered random number using said common key to generate a second random number, generate a session key from said first random number and said second random number, receive a third enciphered number from said security module, decipher said third enciphered number using said session key to generate an authentication test value, and verify that said authentication test value matches said second random number.

Serial No. : 09/992,831

Patent
Docket No. 156906-0010

16. (Currently Amended) ~~[[The]]~~ A security module of claim 6, for use in a gaming device, comprising:

a data device reader interface for connection to a data device reader;
a gaming device interface for connection to a game device processor; and
a processor interposed between said data device reader interface and said gaming device interface, said processor configured to prevent communication between said data device reader and said game device processor unless said data device reader is first authenticated;

wherein said processor is configured to perform a cross-authentication check with said data device reader, and wherein said data device reader is configured to perform a separate cross-authentication check with a portable data device.

17. (Currently Amended) ~~[[The]]~~ A security module of claim 6, for use in a gaming device, comprising:

a data device reader interface for connection to a data device reader;
a gaming device interface for connection to a game device processor; and
a processor interposed between said data device reader interface and said gaming device interface, said processor configured to prevent communication between said data device reader and said game device processor unless said data device reader is first authenticated;

wherein said processor is configured to generate a first random number, encipher said first random number using a common key to generate a first enciphered random number, send said first enciphered random number to said data

Serial No. : 09/992,831**Patent
Docket No. 156906-0010**

device reader, receive a second enciphered random number from said data device reader, decipher said second enciphered random number using said common key to generate a second random number, generate a session key from said first random number and said second random number, receive a third enciphered number from said data device reader, decipher said third enciphered number using said session key to generate an authentication test value, and verify that said authentication test value matches said second random number.

18. (Currently Amended) A method of authentication for use in a cashless system wherein portable data devices may be used to conduct cashless transactions, said method comprising:

reading a portable data device with a data device reader physically proximate to a host device, said host device comprising a host device processor;

performing a cross-authentication between **[[a]]** said data device reader and a security module uniquely identified with said host device when a portable data device is presented to and read by said data device reader, said security module interposed between said data device reader and said host device processor; and

preventing completion of a transaction involving said data device reader and said host device processor unless said data device reader is successfully cross-authenticated with said security module, independent of any authentication of said portable data device by said data device reader.

Serial No. : 09/992,831

Patent
Docket No. 156906-0010

19. (Previously Presented) The method of claim 18, wherein said host device comprises an electronic gaming machine, and wherein said host device processor controls the electronic gaming machine.

20. (Previously Presented) The method of claim 18, further comprising the step of cross-authenticating the portable data device with the data device reader.

21. (Currently Amended) ~~[[The]]~~ A method ~~of claim 18, of~~ authentication for use in a cashless system wherein portable data devices may be used to conduct cashless transactions, said method comprising:

reading a portable data device with a data device reader physically proximate to a host device, said host device comprising a host device processor;

performing a cross-authentication between a said data device reader and a security module uniquely identified with said host device when a portable data device is presented to and read by said data device reader; and

preventing completion of a transaction involving said data device reader and said host device processor unless said data device reader is successfully cross-authenticated with said security module, independent of any authentication of said portable data device by said data device reader;

wherein said data device reader is configured to perform the following steps in connection with cross-authenticating said security module:

generating a first random number at said data device reader;

Serial No. : 09/992,831**Patent
Docket No. 156906-0010**

enciphering said first random number using a common key to generate a first enciphered random number;

sending said first enciphered random number to said security module;

receiving, at said data device reader, a second enciphered random number from said security module;

deciphering said second enciphered random number using said common key to generate a second random number;

generating, at said data device reader, a session key from said first random number and said second random number;

receiving a third enciphered number from said security module, said third enciphered number comprising said first random number having been enciphered by said security module using said session key;

deciphering, at said data device reader, said third enciphered number using said session key to generate a first authentication test value; and

verifying that said first authentication test value matches said first random number.

22. (Previously Presented) The method of claim 21, wherein said security module is configured to perform the following steps in connection with cross-authenticating said data device reader:

generating a second random number at said security module;

enciphering said second random number using a common key to generate said second enciphered random number;

Serial No. : 09/992,831**Patent
Docket No. 156906-0010**

sending said second enciphered random number to said data device reader;

receiving said first enciphered random number from said data device reader;

deciphering said first enciphered random number using said common key to generate said first random number;

generating, at said security module, said session key from said first random number and said second random number;

receiving a fourth enciphered number from said data device reader, said fourth enciphered number comprising said second random number having been enciphered by said data device reader using said session key;

deciphering, at said security module, said fourth enciphered number using said session key to generate a second authentication test value; and

verifying that said second authentication test value matches said second random number